indicating that the claims are not enabled, the Examiner has failed to specify wherein the claims lack enablement. Therefore, there is no *prima facie* case of an enablement rejection.

If the Examiner intended a rejection under the "written description" requirements of 35 USC 112, first paragraph, Applicants indicate that the specification clearly provides support for the phrase "communication protocol layer independent security." The title of the invention is "LAYER-INDEPENDENT SECURITY FOR COMMUNICATION CHANNELS." The only layers referred to in the specification are "communication protocol layers." Page 4, lines 2 and 3 of the specification refer to "communication protocol-independent security." On page 5 of specification, the brief description of Figure 4 refers to a "layer-independent secure communication in a multi-layered communication network." Page 6 of the specification, lines 2 and 3, refer to "layer-independent secure communications in a multi-layered communication network." Thus, the phrase "communication protocol independent security" has support within the specification. The layer independent security of the specification is contrasted with "layer-specific" encryption on pages 2 and 3 of the specification. Again, the only layers referred to in the specification are communication protocol layers. Therefore, there is ample support in the written description of the invention for the use of the phrase "communication protocol layer independent security." Nevertheless, the Examiner feels the phrase should be utilized expressly in the specification, Applicants offer to amend the specification to include that specific phrase.

The Examiner rejected claims 1, 2, 5, 6, 13, 14, 17, 20, 21, 24, 25, 28, 29, 32, and 33 under 35 USC 102(e) as anticipated by Elgamal. The Examiner states:

> "In line 7 of column 14, Elgamal discusses transmitting data is [sic - in?] streams. This anticipates steps a-c, all of which are apparent from communicating via data streams. He goes on in the following paragraph to discuss encryption in the application layer. The application layer is the top layer, and as such, is not dependent upon any other layers. Decryption at a recipient is anticipated by an encryption. This anticipates the last three steps."

The Examiner's application of Elgamal reflects a misreading of the term "stream". When talking about banking transactions, Elgamal says "it might be acceptable to encrypt the bulk of the data using one of the algorithms currently approved for export, however, the financial data should be protected at an acceptable level... regardless of the geographical location." This appears to be a reference to the fact that only weak encryption algorithms are approved for export outside the U.S. Therefore, additional encryption of the encrypted data may be necessary in order to protect the financial data. The reference in column 15, line 7 to "other data streams" appears to be a reference to sources of financial data coming from other banks to be multiplex for international transmission. The paragraph beginning column 15, line 9, talks about encryption "within a message." "Individual field encryption" is not stream data. Similarly, "channel encryption" is communication channel data such as that accomplished at the various layers of a communication protocol.

It is important to interpret the phrase "stream" in a way which is consistent with the specification, rather than at odds to it. For example, one would not interpret "stream" in the context of this application as referring to a flow of water down a mountain side. On page 4 of the specification, beginning line 9, the application states that a "stream" is an abstraction which refers to the transfer or "flow" of data, in any format, from a single source, to a single destination. Let us consider the following example in the context of Figure 1 of the application. Let us assume that process 108 is an MPEG2 transmission process. It may generate a plurality of "streams", such as a left channel audio, a right channel audio, a video, a closed-captioned stream, and a control channel stream. When the MPEG2 transmission process 108 desires to send information to process 110, which, in this example, is an MPEG2 display process, a communications channel would be set up between node 108 and node 104 then, the individual streams would be applied to the communications channel for transmission to the node 104. Note that the communication channel from the process 108 goes through all of the layers shown in Figure 1 of each protocol stack, namely the application layer, presentation layer, session layer, transport layer, network layer, datalink layer, and physical layer before going across the transmission medium to the other node and then passing through the same layers as an inverse order. It is known in the art to apply layer specific encryption at any of the layers of the OSI reference model shown in Figure 1.

If the invention of claim 1 were applied to a communication system which corresponded to the OSI reference model, first, communications would be established between the first network node and the second network node. The request for connection would come from the process 108 to the application layer and appropriately process through the layers until a connection is set up to node 104. Once that is done, a first stream, say, for example, an MPEG control channel stream is established between the first process 108 and the communications channel which begins at application layer 118. At the other end, a stream would be established between the application layer 128 of node 104 and the process 110 for the MPEG control channel data. As set forth in limitation d) of claim 1, in response to data being written to the first stream [from process 108] the data is encrypted to generate encrypted data which is then applied to the application layer 118. The encryption is performed independently of any of the layers of the communications protocol stack. Note that in the example of MPEG2, encryption can be applied selectively to the streams rather than to everything that is transmitted over the communications channel. In OSI reference model, the layer normally responsible for encryption is the presentation layer. The application layer, 118, handles the interface between the software involved with the process 108 and the communications channel.

Limitation f) of claim 1 states "in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover the decrypted data."

Elgamal does not anticipate the claims because it doesn't first establish a communications channel and then establish streams linking from the first process to the channel and a second stream from the communications channel to the second process. Further, Elgamal's encryption is not "layer independent." The Examiner states "the application layer is the top layer, and is such not dependent upon any other layers." The Examiner appears to misapprehend the function of the application layer. The application layer serves as an interface between the software process 108 and the layers of the protocol stack. Encryption at the application layer is layer dependent because it is done in one of the layers of the protocol stack.

A stream is an abstraction, which has properties beyond merely being a string of binary digits. "Streams" are defined in object oriented languages such as Java and have a whole set of properties that distinguish them from an arbitrary string of binary 1's and 0's and which distinguish them from a flow of water down the mountain side.

Neither Elgamal nor the other references teach or suggest the use of a "stream" as that term was used or applied in the specification and claims of this application.

Thus, the Examiner has failed to establish a *prima facie* case of anticipation of the claims when the claims are properly interpreted.

The Examiner rejected claims 1, 5, 13, 17, 20, 24, 28 and 32 under 35 USC 102(e) as anticipated by Helwig et al. The portion of the specification of Helwig et al. relied upon by the Examiner refers to Figure 3 and, more particularly, to a "pre-transmit process 68" within Figure 3. The whole purpose of that particular branch coming off of 66-y is to record a test message in memory. There is no teaching or suggestion of first establishing a communications channel and then establishing streams to that channel and streams from that channel which are independently encoded independently of protocol layers. Helwig et al. does refer to a "data stream" but that does not correspond to the "stream" abstraction of the application. Rather, it is a series of bits output from a vocoder.

Thus, the Examiner has failed to establish a *prima facie* case of anticipation of these claims over the Helwig et al. reference.

The Examiner rejected claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC 102(b) as anticipated by Schneier (Applied Cryptography). Schneier describes an XOR encryption process with it's corresponding decryption process. There is no establishment of a communications channel followed by establishing a stream between a process and the channel and another stream from the channel to an output process. Thus, the Examiner has failed to establish a *prima facie* case of anticipation. In addition, the Examiner fails to show any teaching or suggestion of using a "stream" as described in this application. Thus, the Examiner has failed to establish a *prima facie* case of anticipation based on the Schneier (Applied Cryptography) reference.

The Examiner rejected claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27, 30, 31, 34 and 35 under 35 USC 103(a) as unpatentable over Elgamal, Schneier, or Helwig et al. Referring to these claims, the Examiner states: "They do not say that the communication channels or data streams are Java-based. Official notice is taken that it is old and well-known that Java is intended for networked/distributed environments and enables the construction of virus-free, tamper-free systems. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to base the systems of Elgamal, Schneier, or Helwig et al., all of which are networked or distributed environments, on Java, as is known in the art. This would enable the implementation of a virus-free, tamper-free system."

If the Examiner were to implement the Elgamal, Schneier or Helwig et al. systems, using Java streams and Java secure channels, it would still not result in the claimed invention. In fact, if the phrase "communication channel" and "stream" as used in the references is interpreted to be a "Java stream" and "Java secure communication channel," the interpretation of the references as applied to the independent claims would have to change so dramatically as to show their inapplicability under 35 USC 102.

The Examiner rejected claims 2, 6, and 14 under 35 USC 103(a) as unpatentable over Helwig et al. or Schneier. The problems with these rejections have been discussed in conjunction with the parent claims.

There are several benefits achieved by the claimed invention. These are set forth, for example, on pages 2 and 3 of the specification. When the amount of information included in session is small, for example, when a session contains only a single message, then the overhead contributable to set up negotiation can adversely affect communications performance. This negative is overcome by the claimed invention. Further, some communication architectures do not include a session layer, which requires that a session layer be added to support session type security, further degrading performance. Layer specific encryption can avoid the overhead penalty associated with set up negotiation, but it has additional limitations. First, encryption and decryption must occur at the same corresponding layer on both the transmitting and receiving network nodes. The traditional techniques such as the simple key management for internet protocols (SKIP) and secure sockets layer (SSL) each require layer specific function calls. The result is that one application implementing security according to SKIP cannot interact with another application implementing security according to SSL. In addition, layer-specific encryption could be difficult to employ an object-oriented environments because of the inherent level of abstraction required. For example, some layers operate of databytes, which often is a much lower level than objects in an object oriented environment.

The references applied by the Examiner, even if modified as suggested by the Examiner, would not result in achieving these benefits.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current Amendment. The attached pages are captioned "Version With Markings to Show Changes Made".

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Gene Z. Rubin 33,351

for David L. Stewart
Registration No. 37,578

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 DLS:kap
Date: May 14, 2001
Facsimile: (202) 756-8087

WDC99 424693-1.050435.0015